Instructor's Guide to Accompany
NETWORK DEFENSE AND COUNTERMEASURES

CHAPTER 2
TYPES OF ATTACKS

CHAPTER OBJECTIVES

When students have finished reading this chapter, they will be able to:

- Describe the most common network attacks including session hacking, virus attacks, Trojan horses, denial of service, and buffer overflow.
- Explain how these attacks are executed.
- Identify basic defenses against those attacks.
- Configure a system to prevent denial of service attacks.
- Configure a system to defend against Trojan horse attacks.
- Configure a system to defend against buffer overflow attacks.

CHAPTER OVERVIEW

This chapter examines the most common types of attacks made on computer networks and explains how such attacks are executed. Special attention is paid to denial of service attacks because it is a common Internet attack method. The chapter also details other common attacks, including IP spoofing, session hacking, virus attacks, Trojan horses, and buffer overflow attacks. The student learns how to configure a system to defend against these specific threats.

CHAPTER OUTLINE

1. Introduction
2. Understanding Denial of Service Attacks
3. Defending Against Buffer Overflow Attacks
4. Defending Against IP Spoofing
5. Defending Against Session Hacking

6. Blocking Virus and Trojan Horse Attacks

7. Summary

TEACHING NOTES AND TIPS PER TOPIC

1. Introduction

Teaching Tip: Tie the first chapter into this chapter by asking students to identify the three classifications of attacks identified in Chapter 1 (Intrusion, Blocking, and Malware). While the first chapter discussed general categorizes of threats, this chapter focuses deeper into specific types of attacks and ways to defend against them.

2. Understanding Denial of Service

Teaching Note: This section describes various types of DoS attacks and techniques for preventing them. There is opportunity for hands-on exploration and/or instructor demos. To perform the steps in the *DoS in Action* section, files must be downloaded. Plan and test your classroom network configuration ahead of the lesson.

Topics include:

- DoS in Action
- SYN Flood
- Smurf Attack
- Ping of Death
- UDP Flood
- ICMP Flood
- DHCP Starvation
- HTTP Post DoS
- PDoS
- Distributed Reflection Denial of Service
- DoS Tools
- Real-World Examples
- Defending Against DoS Attacks

Teaching Tip: To help students understand the way DoS attacks work and the kind of disruption they can cause, review some recent examples of real-world DoS attacks. Discuss the types of operational limitations that render virtually any network vulnerable to this threat.

Teaching Tip: To help students grasp the potential scope of a major DoS attack, tell students that a well-distributed virus can spread to tens or hundreds of thousands of systems. If the virus is programmed to launch a DoS attack at a specific date and time, all the "hijacked" systems attack the target at the same time. This can result in millions of data packets flooding the target system bringing it to a halt.

Teaching Tip: Because viruses and Trojan horses can be used as the basis for several kinds of DoS attacks, it is essential that every computer on a network (especially servers) have antivirus software installed. It is equally important to make sure that the antivirus programs are kept updated and active.

Teaching Tip: Have a lab system preconfigured so that students can perform the example outlined in the "DoS in Action" section. This lab requires downloading and installing server software. Plan, test, and adjust this lab to adhere to your classroom network security. If time allows, let students perform the example themselves. Make sure students know that they should not perform such exercises on their own computers or on "live" systems belonging to an organization. Labs of this type may shut the system down, so they should be performed only on a computer or network that is set up specifically for this purpose.

Teaching Tip: If possible, download and install a popular DoS tool (such as TFN or Trin00) on a lab machine so that students can explore it and learn how it can be used. If this is possible, and if schedule allows, assign students to prepare a brief paper or presentation on one aspect of the program. Ask students to share their findings with the entire class.

3. Defending Against Buffer Overflow Attacks

Teaching Note: This section explains what a buffer overflow is, how it can be used by an attacker, and how to prevent such an attack.

Teaching Tip: Use Figure 2-7 as a visual for discussing a buffer overflow attack.

Teaching Tip: Lead a discussion about why the buffer overflow attack is slightly less prevalent than a DoS attack. (DoS typically involves knowing how to write code in a compiled language such as C or C++.) Contrast this to the ease of adding a simple scripting, or macro virus to a Word document. Demonstrate by opening a scripting window in Microsoft Word and explain that scripting code is embedded here in the Word document and can be easily attached to an e-mail. (If you do not see the developer tab to open a scripting window, follow instructions here https://docs.microsoft.com/en-us/visualstudio/vsto/how-to-show-the-developer-tab-on-the-ribbon). There is no need to write script in this demo. Opening the scripting window and demonstrating where the code is written and explaining that the code is distributed with the document as "hidden" content is sufficient.

Teaching Tip: If you or any students have programming expertise, write a simple example of code that utilizes a buffer. (It is only necessary to write the code on a whiteboard so that students can see it.) Show students this example and explain how it functions to help them understand how programs use buffers and how this can be exploited by an attacker.

4. Defending Against IP Spoofing

Teaching Note: This section examines how hackers can hide their own IP address when attacking other computers and identifies a simple defense against being "spoofed."

Teaching Tip: Extend the discussion to DNS hijacking. DNS hijacking is the practice of rerouting one's Internet browsing so traffic can be monitored or redirected. Have students run the F-Secure Router Checker tool, or a similar tool, to check for signs of DNS hijacking. You can find the tool here https://www.f-secure.com/en/web/labs_global/router-checker .

5. Defending Against Session Hacking

Teaching Note: This section explains how a hacker can take over a TCP session between two computers, and how administrators can thwart this type of hacking.

Teaching Tip: Ask students to describe the kinds of tasks a hacker might perform during session hacking. For example, might a hacker use this technique to intercept e-mail messages being transmitted between e-mail servers?

Teaching Tip: Explain that there are many vendors that manufacture filtering routers, such as D-Link and Cisco. Ask students to perform a quick Internet search on "Top Filtering Routers" for the current year. Create a group list and identify the top three that appeared most often.

6. Blocking Virus and Trojan Horse Attacks

Teaching Note: This section provides examples of major virus attacks and the damage they cause and describes simple strategies for preventing viruses from reaching your system.

Topics include:

- Viruses
- Types of Viruses
- Trojan Horses

Teaching Tip: Make sure that students understand the distinctions between viruses, worms, and Trojan horses. In some cases, these distinctions are slight, but it is important to know them to properly differentiate these classes of threats.

Teaching Tip: Viruses can do much more than replicate themselves and send e-mail messages. Lead students in a discussion of the many types of damage viruses can do. Create a list on the whiteboard and ask students to contribute to it.

Teaching Tip: It would be helpful if network administrators could look into the minds of virus writers, but as the text discusses, little is actually known about the motivations of virus writers. Lead students in a discussion about such motivations. If a student could write a virus, what would it do? What kind of damage would it cause? What reason would the student have for turning it loose?

Teaching Tip: Have any students' computer ever been infected by a virus? Ask students to recount their experiences with viruses. What kinds of damage did their systems suffer? How could they have prevented the virus from infecting their systems? What lessons did they learn, and how did the experience change the way they manage their computers?

Teaching Tip: It's important for students to know that new threats surface every day. While it is impossible to know each new threat, there are many sites that can be used to identify and troubleshoot threats. Group students together and assign them a classification such as: virus, worm, Trojan horse, or spyware. Using a site such as https://www.f-secure.com/en/web/labs_global/threat-descriptions, have each group research a latest threat in their assigned category. Have students report to the class the name, description, and characteristics of the threat.

ACTIVITIES FOR CLASS

I. Discussion Questions

A. Discussion Question 1

As you learned in Chapter 2, one way to secure a network from attack is by blocking all incoming traffic. But is such a measure practical? Imagine running a network in different types of

organizations (a bank, a university, and others). Would this be the ideal way to protect the organization's network from attack? Why or why not?

Answer: Students' answers may vary. There should be a discussion of the importance of various kinds of traffic to different types of organizations. For example, many banks offer online services to customers, making inbound traffic essential. But the same might not be true for a small business such as a shoe store. Students should also discuss other types of security measures that should be taken when traffic blocking is not practical.

B. Discussion Question 2

Perhaps you have seen the TV commercial in which a bored office worker unthinkingly opens an e-mail message, which launches a virus on her computer. The virus immediately spreads to her coworkers' computers and chaos breaks out in the office. The commercial may be overly dramatic (or comic, depending on your point of view), but it raises an important question: Should a worker be held responsible for bringing a virus into an organization's network, even by accident? If so, what penalties would be reasonable? How can organizations prevent such incidents?

Answer: Students' answers will likely vary, but the discussion here should focus on the accountability of users for creating such problems and the methods managers can employ to prevent these problems. Steer the discussion away from technological solutions, helping students concentrate on Human Resources and policy-related solutions.

II. Web Projects

A. Web Project 1

Divide the class into groups and ask each group to study Blaster, MyDoom, W32.Storm, or Slammer. Each group should prepare a brief presentation to share with the entire class. Each group's presentation should focus on the extent of damage caused by the worm and examine deterrents that could have stopped the worm from spreading. Ask students to analyze this question: In each case, why didn't users and administrators take stronger steps to avoid infection or to prevent the worm from spreading?

Answer: Students' answers will vary, depending on the resources they use.

B. Web Project 2

Visit a variety of security-related websites and try to find a startling statistic on attacks and threats.

Answer: Students' answers will vary, depending on the resources they use. If students need guidance in finding a reliable resource, have them search for "Symantec ISTR Report" for the current year. Symantec produces an Internet Security Threat Report each year, that includes an introductory page of statistics. Successful students will learn that attacks are common and remain on the rise, affecting organizations of all sizes, not just large corporations.

C. Web Project 3

Search the United States Computer Emergency Readiness Team (US-CERT) website at http://www.us-cert.gov/ for information about buffer overflow attacks. How many programs or operating systems can you identify that are vulnerable to this type of attack?

Answer: Students' answers will vary, but every student should show evidence of having done a thorough search of the site. US-CERT has catalogued a number of buffer overflow vulnerabilities in a variety of software programs and has issued warnings about many of them. These warnings generally include technical details about the program as well as procedures for fixing them.

D. Web Project 4

Using your favorite search engine, such as Google (http://www.google.com/) or Yahoo! (http://www.yahoo.com/), do some research on monitoring programs. How do such programs work? Are they specifically for certain types of networks or operating systems? Which one would be most useful in a given environment? Be prepared to share your findings with the class.

Answer: Students' answers will vary but should show evidence of thorough, independent research using any online sources they can find. Students should have a good idea of how these tools work and in which environments they might be most useful.

E. Web Project 5

Do you know how to update an antivirus program? Many commercial antivirus programs can automatically update themselves if the user subscribes to this service. Even so, most AV programs can be updated manually by visiting the vendor's website, finding the update instructions for your product, and following the required steps. Visit the website of the AV program that is installed on your lab or home PC, and update it manually. Write a paragraph that describes your experience.

Answer: Successful students will determine which antivirus program is installed on their PC, locate the vendor's website, and manually download the latest updates to the program. The difficulty of this task will depend on the program, the vendor, and the types/number of updates available. Students should describe the process, the difficulty level, any problems encountered, and their ultimate success or failure.

WEB RESOURCES

- http://www.247.prenhall.com/ Pearson product support
- http://www.us-cert.gov/ The United States Computer Emergency Readiness Team site; a respected security resource provided by the U.S. Department of Homeland Security
- http://www.f-secure.com/virus-info/virus-news/ An authoritative clearinghouse of information about viruses
- https://www.f-secure.com/en/web/labs_global/threat-descriptions An authoritative list of latest attack threats
- http://www.sarc.com/ The Symantec Security Response website, filled with up-to-date information on current virus threats and information on updating Norton Security products

- http://www.denialinfo.com/dos.html A list of informative resources on denial of service attacks

- https://www.giac.org/paper/gsec/1483/hyperlink-web-spoofing-identifying-defending-hacker-attacks/102766 SANS Institute White Paper on Hyperlink and Web Spoofing

UCERTIFY

If you are using the uCertify course and labs product, be sure to review the associated online labs for this chapter. Students can do these labs as homework or during class time for hands-on practice to reinforce core learning objectives.